IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

UNITED STATES OF AMERICA,	§	
	§	
Plaintiff,	§	
	§	
v.	§	Case No. 1:24-CV-00798-ADA
	§	
SOUTHWEST KEY PROGRAMS, INC.,	§	
	§	
Defendant.	§	

ORDER REGARDING ELECTRONICALLY STORED INFORMATION

The Parties have entered into a stipulation governing electronically stored information ("ESI") and requested that the Court enter it as an order. Rule 26(f) of the Federal Rules of Civil Procedure requires the Parties to develop a proposed discovery plan that states the parties' views and proposals on, among other things, "preservation of electronically stored information, including the form or forms in which it should be produced." Fed. R. Civ. P. 26(f)(3)(C). On December 20, 2024, the Parties filed a joint discovery plan in which the Parties agreed to jointly file a stipulation governing preservation and production of ESI by February 21, 2025. The Parties have conferred and agree to the following protocols governing ESI.

It is hereby ORDERED:

1. **Limitations on Obligation to Preserve and Produce**: Subject to Paragraph 3(a), for purposes of this action, the Parties agree to limit the scope of preservation as described in this section.

   a. The Parties agree that they do not need to take specific, affirmative steps to preserve for purposes of this litigation the following categories of ESI:

      i. Delivery or read receipts of e-mail;

ii. Logs or other data from video-conferencing (including, *e.g.*, Skype or Zoom);

iii. Instant messaging tools (*e.g.*, Slack, Teams chat) among (i) attorneys for the United States (and their staff) or (ii) attorneys for Southwest Key Programs, Inc. ("Southwest Key") (and attorneys' staff) including both in-house and outside counsel.

iv. Temporary or cache files, including internet history, web browser cache, and cookie files, wherever located;

v. Internally facing server system logs;

vi. Externally facing or hosted file sharing system logs;

vii. System data from photocopiers or fax machines;

viii. Auto-saved copies of electronic documents;

ix. Deleted, slack, fragmented, or other data only accessible by forensics;

x. Random access memory ("RAM"), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system;

xi. Logs of or other data from audio calls (including, *e.g.*, landline phones, mobile devices, and Voice Over Internet Protocol ("VOIP")) made to or from (i) attorneys for the United States (and their staff) or (ii) attorneys for Southwest Key (and attorneys' staff);

xii. Voicemail messages and text messages on the voicemail systems of (i) attorneys for the United States (and their staff) or (ii) attorneys for Southwest Key (and attorneys' staff) including both in-house and outside counsel;

xiii. Data in metadata fields that are frequently updated automatically, such as

last-opened dates;

xiv. Back-up data that are substantially duplicative of data that are more accessible elsewhere;

xv. Server, system or network logs; and

xvi. Data remaining from systems no longer in use that is unintelligible on the systems in use.

b. When duplicate copies[1] of relevant ESI exist in more than one location, this Plan does not require a Party to preserve all duplicates as follows:

i. ESI existing or stored on mobile or portable devices (*e.g.*, smartphones, tablets, thumb drives, CDs, DVDs, etc.) or file sharing sites does not need to be preserved pursuant to this Plan *provided that* duplicate copies of the ESI, including metadata, are preserved in another location reasonably accessible to the Party.

ii. ESI on backup tapes, continuity of operations or disaster recovery systems, data or system mirrors or shadows, and other systems that are used primarily for the purpose of system recovery or information restoration and are not reasonably accessible ("Backup Systems") need not be preserved pursuant to this Plan *provided that* duplicate copies of relevant ESI have been preserved in another reasonably accessible location. However, if a Party knows that relevant ESI exists *only* on a Party's Backup System, the Party will take reasonable steps to preserve ESI on the Backup System until the

[1] "Duplicates" in the context of ESI are copies of identical documents identified with matching MD5 hashes, which is a mathematically-calculated 128-bit value used to create a unique identifier for an electronic file.

Parties can agree on how and when the ESI will be preserved or produced. If the Parties cannot reach agreement, they will seek a ruling from the Court.

c. The Parties agree that they do not need to take specific, affirmative steps to preserve for purposes of this litigation relevant documents, things, or ESI (including internal communications, drafts, versions, and collaboration on case-related work) created by and, if shared with any other(s), exchanged *solely among*: 1) attorneys for the United States (and their staff); or 2) attorneys for Southwest Key (or attorneys' staff), including in-house and outside counsel; or 3) the United States (and their staff) and attorneys for the U.S. Department of Health and Human Services and/or Office of Refugee Resettlement.

d. The Parties agree not to seek discovery of documents, things, and ESI that they have agreed not to preserve pursuant to Paragraph 1(a)-(c) above. As provided in Paragraph 3(a) below, the Parties do not need to list such items on a privilege log prepared and served in connection with discovery in this case.

2. **Identification & Production of Documents, Things, and ESI**

a. Production Format

i. ESI and hard copy paper documents will be produced as specified herein.

ii. Each hard copy paper document must be scanned and produced in electronic form as specified herein.

iii. Except as provided in Paragraph 2(a)(xv) below, ESI must be processed with eDiscovery software that extracts metadata and text and converts the document to image format that accurately represents the full contents of the document.

iv. For ESI and scanned hard copy paper documents, black and white content

shall be scanned or converted to single page Tagged Image File Format ("TIFF"), using CCITT Group IV compression at 300 d.p.i. and that accurately reflects the full and complete information contained in the original document. One image file shall represent one page of the document. Color content shall be produced as JPEG files at 300 d.p.i. using a high-quality setting. Nothing in this provision prevents a Party from scanning, converting, and/or producing documents or content as color images.

v. For ESI and scanned hard copy paper documents, the text of all pages in the document must be saved as one file. If the extracted text of a native document does not exist or does not represent the entire document, Optical Character Recognition ("OCR") will be provided instead.

vi. Metadata must be preserved and produced for the fields listed in Appendix A.

vii. Deduplication will be used to remove exact duplicate documents from the production at the family level: *i.e.*, the Parties will take reasonable steps to not remove or delete attachments even if duplicated elsewhere in the production. The Parties agree to use MD-5 hash values for deduplication and calculate those values for all ESI at the time of collection or processing globally across custodial data.

viii. Use of Search Criteria to Identify ESI: It is the responsibility of the Party responding to a discovery request to identify and produce responsive information including ESI. The Parties agree to meet and confer if either believes that the use of keyword search criteria or analytic tools should be

used to identify responsive ESI.

ix. All productions will provide a consistent load file with the same number and order of fields regardless of the types of documents in the production.

x. All images (e.g., TIFF, JPEG) will be produced in a directory labeled IMAGES. Subdirectories may be created so that one directory does not contain more than 5000 files.

xi. All native files (with the proper Windows-associated extension) will be produced in a directory labeled NATIVE. Subdirectories may be created so that one directory does not contain more than 5000 files. The Parties agree that native files will be provided for only those non-privileged, unredacted documents of file types identified for native production in 2(a)(xv).

xii. An image cross reference file (a file in Concordance Opticon/Relativity .log format that contains Bates Numbers, paths to images, and document break indicators for all ESI in each production) and a load file containing all required metadata fields will be produced in a directory labeled DATA.

xiii. All extracted text and/or OCR will be produced in a directory labeled TEXT. OCR is searchable text generated for scanned documents or native files that is in ASCII format, where all pages in the document will be represented in one file. The parties agree to provide a text file for all documents, even if the size of the file is zero. Subdirectories may be created so that one directory does not contain more than 5000 files.

xiv. Except for native files, the Parties will produce responsive documents Bates-stamped with a prefix to indicate the Party producing the documents

(e.g., "US" and "SWK"). For native files, which cannot be Bates-stamped, the Parties will rename the file as [Document Identification Number].[extension] with a placeholder image in the production containing the original name of the file.

xv. Specifications for Specific File Types:

(a) Text messages may be produced initially as Relativity Short Message Format or may be produced as PDFs of screen shots, with each conversation produced as a single file, including all sent images/attachments.

(b) Audio files and video files shall be produced as native files unless the native form is a proprietary format, in which case the file(s) should be converted into a non-proprietary format that can be played using Windows Media Player. For each audio or video file, a placeholder image containing the file name shall be included in the production.

(c) Excel or other types of spreadsheets shall be produced as native files without password(s) or produced as native with password(s) provided contemporaneously for the entire workbook(s). For each Excel or spreadsheet file, a placeholder image containing the file name shall be included in the production.

(d) PowerPoint files shall be produced as native files with all notes unaltered and viewable. For each PowerPoint, a placeholder image containing the file name shall be included in the production.

(e) Social media content (including comments, "likes," sharing, and

other interactions with the post(s)) should be produced as individual images with extracted text, including information about the participants and the date and time of the communications.

(f) For production of tangible things and production of information from a structured database, proprietary software, vendor-managed software, or other source from which native production is not reasonably practicable, the parties will meet-and-confer before making any production to attempt to agree on a reasonable and proportional form of production that maintains the integrity of the tangible things or documents.

(g) Oversized documents (*e.g.*, architectural, engineering, or zoning plans) must be produced as JPEG images, PDF Files, or in hard copy paper form so as to retain the resolution and scale of the original document.

b. Production Specifications

i. Responsive documents and ESI will be produced via password-protected .zip file(s) uploaded to an electronic file transfer site, in accordance to the written instructions provided by counsel for the Requesting Party or as otherwise agreed by the Parties. The password shall be communicated in a separately-transmitted email. In the case of documents and ESI produced by the United States, responsive information will be produced via .zip file(s) uploaded to the Justice Enterprise File Sharing System (JEFS) or USAfx File Exchange.

ii. Productions via electronic file transfer will be uploaded in a manner (or

otherwise clearly labeled) to indicate (1) the Party producing the information, (2) the date of the production, and (3) the Bates-range(s).

iii. If a Party needs to redact a portion of a document for which only a native file would be produced, the Party may produce an imaged version of the redacted documents, or produce the document in another form as agreed by the Parties.

iv. The Parties agree to remove all encryption or password protection for all ESI produced. In the alternative, the Parties agree to provide passwords or assistance needed to open encrypted files.

3. **Privileged Documents, Things, and ESI**

a. If any discovery request appears to call for the production of documents, things, or ESI covered by Paragraph 1, the responding Party is not required to produce or identify such information on a privilege log. However, if a Party preserves relevant documents, things, or ESI covered by Paragraph 1 in order to support a claim or defense in this case, the Party shall produce such information or identify it on a privilege log notwithstanding this subsection.

b. Each Party's privilege log must provide sufficient information for the receiving party to assess the producing party's claim of privilege. The privilege log may provide the available objective metadata outlined in Appendix A (to the extent it is reasonably available and does not reflect privileged or protected information) and an indication of the privilege or protection being asserted. With respect to the "Subject" or "Native_filename" field, the producing Party may substitute a description of the document where the contents of these fields may reveal privileged information. In the privilege log(s), the producing Party shall identify

each instance in which it has modified the content of the "Subject" or "Native_filename" field.

c. Following the receipt of a privilege log or redacted documents, a requesting Party may identify, in writing (by Bates/unique identified number), the particular documents that it believes require further explanation. Within thirty (30) days of such request, the producing Party must either (i) provide the requested information or (ii) challenge the request. If a Party challenges a request for further information, the Parties shall meet and confer to try to reach a mutually agreeable solution within thirty (30) days of any such challenge and prior to seeking any relief from the Court.

d. Redactions should be narrowly tailored to protect only privileged information and not underlying facts. Documents with narrowly tailored redactions need not be logged as long as (i) for emails, the objective metadata (i.e., to, from, cc, bcc, recipients, subject, attachments, date, and time, unless the privilege or protection is contained in these fields) is not redacted, and the reason for the redaction, including the nature of the privilege asserted, is noted on the face of the document; and (ii) for non-email documents, the reason for the redaction is noted on the face of the document in the redacted area, along with identification of the author, all senders of the document, all recipients of the document, and the date of the document. Documents that are substantially redacted where the subject matter is not decipherable should be logged along with a description of the contents of the document that is sufficient to understand the subject matter.

e. <u>Disclosure of Privileged or Protected Information</u>

    i. The production of privileged or work-product protected documents, ESI,

or information (collectively "materials"), whether inadvertent or otherwise, is not a waiver of the privilege or protection from discovery in this case or in any other federal or state proceeding. This Order shall be interpreted to provide the maximum protection allowed by Federal Rule of Evidence 502(d).

ii. Notwithstanding the foregoing, a Party waives all claims of privilege or protection of materials if the material was used in this action by any Party in a deposition, expert report, court hearing, or court filing (excepting a motion related to a disputed privilege claim) and the producing Party does not make a written request for return of the material ("Clawback Notice") within 5 days of the initial use of the document(s). Failure to timely clawback used material waives all claims of privilege or protection as to the material in this action but does not operate as a subject matter waiver.

iii. If the producing Party discovers that it disclosed information that it asserts is privileged or protected, it will issue a Clawback Notice to the receiving Party within 21 days of the date of discovery and provide the production date, number, and volume of the disc or drive on which the production was produced ("production media"), and the Bates number(s) or Document ID (for native files) of all material that it believes contains the privileged or protected information.

iv. If a production contains information that the receiving Party believes is privileged or protected, it will notify the producing Party within 21 days from the date of discovery and provide the Bates number(s) or Document ID (for native files) of the material it believes is privileged or protected.

Within 21 days after receiving the notification, the producing Party may provide a Clawback Notice. If the producing Party does not send a Clawback Notice to the receiving Party within 21 days, the producing Party waives all claims of privilege or protection as to the material in this action, but failure to timely clawback does not operate as a subject matter waiver.

v. Any time a producing Party provides a Clawback Notice, it will also provide either (a) a new copy of the material (utilizing the same bates number or Document ID as the original material) with the privileged or protected material redacted, or (b) a slip sheet noting that the document has been withheld, if the producing Party claims that the entire document is privileged or protected. Within 14 days of the Clawback Notice, the producing Party must provide the receiving Party with a corresponding privilege log and, if the receiving Party must destroy or delete production media (*e.g.*, CD, DVD, thumb drive, or downloaded file(s)) to destroy or delete privileged or protected material, the producing Party will also provide the receiving Party a duplicate copy of the production media minus only the privileged or protected material.

vi. When the receiving Party receives a Clawback Notice, it will make reasonable, good faith efforts to promptly sequester, return or destroy all material identified by the producing Party. If copies of privileged or protected materials are located or stored on the receiving Party's Backup System(s), those copies need not be affirmatively removed, rather, the receiving Party may overwrite those copies according to its normal

records management procedures.

vii. If the receiving Party intends to challenge the claim of privilege or protection, it will keep one copy of the privileged or protected material in a sealed envelope or location(s) sequestered from the case team while seeking a ruling from the Court. Nothing in this Section prevents access by a receiving Party's information technology or security personnel from accessing, in the normal course of their work, systems or locations where privileged or protected material is sequestered.

4. **Costs of Document Production:** Each Party shall bear the costs of producing its own documents, things, and ESI.

SIGNED on February 24, 2025.

ALAN D. ALBRIGHT
UNITED STATES DISTRICT JUDGE

APPENDIX A

Field Name	Definition	Include for Emails and Text Messages	Include for other electronic files	Include for Paper documents
Begin_Bates	Bates number for the first image of a document (or the Bates number of the placeholder page for a native document).	Y	Y	Y
End_Bates	Bates number for the last image of a document (or the Bates number of the placeholder page for a native document).	Y	Y	Y
Begin_Attach	Only for document families,[2] provide Bates number for the first image of the first attachment or embedded file. Leave this field blank if there is no document family.	Y	Y	Y
End_Attach	Only for document families, provide Bates number for the last image of the last attachment or embedded file. Leave this field blank if there is no document family.	Y	Y	Y
Parent ID	Bates number of the parent document (filled in only for "child" documents).	Y	Y	Y
PgCount	The number of images produced for this document (1 for placeholder).	Y	Y	Y
All Custodians	Name of all custodians who had a copy of the document before deduplication.	Y	Y	Y
From	"From" field in email.	Y		
To	"To" field in email.	Y		
CC	"CC" field in email.	Y		
BCC	"BCC" field in email.	Y		
Subject	"Subject" field in email.	Y		
Attachments	File names of the attachments.	Y		
DateSent	DateSent field from email. Include both date and time (format: 9/28/2012 1:16 PM or 9/28/2012 13:16:34).	Y		
Redacted	"Yes" if the document has been redacted.	Y	Y	Y
Confidential	Confidential Designation (if any).	Y	Y	Y
MD5Hash	The MD5 hash value calculated when the file was collected or processed.	Y	Y	
Orig_File Paths	Path to location from which original file	Y	Y	

[2] Document Family means a group of related documents, including: (1) paper documents that were grouped together or physically attached by clips, staples, binding, folder, etc.; (2) email with its attachment(s); and (3) files with embedded documents

	was collected. If production was deduplicated, include all file paths from which original files were collected.			
Prod_FilePath	The path to the native file on the production media.		Y	
Native_filename	Original name of the native file when the file was collected or processed.	Y	Y	
Text File Path	Path to the text file on the production media.	Y	Y	Y
Date File Created	The date the ESI was created.		Y	
Date File Last Modified	The date the ESI was last modified.		Y	